Release notes for

Entrust/PKI™ 6.0.1

Entrust/Authority:
For Microsoft® Windows® 2000 Server (SP1, SP2, SRP1), Windows NT® 4.0 (SP5, SP6, and SP6a)

Entrust/RA:
For Microsoft Windows 2000 Professional, Windows 2000 Server (SP1, SP2, SRP1), Windows NT 4.0 (SP5,SP6, SP6a), and Windows 98

Date: June 21, 2002
Release: 6.0.1 Commercial

Attention: This release contains important improvements to the product's stability and, accordingly, it is recommended that this update be deployed into your production environment as soon as possible.

This document contains release notes for both Entrust/PKI 6.0.1 and 6.0. Please note that some of the known issues in Release 6.0 have been solved in Release 6.0.1. See "Problems solved in Entrust/PKI 6.0.1" on page 8.

Attention: Before you install or upgrade Entrust/PKI or any of its components, check at least the following sections of this release note for critical information about Entrust/PKI 6.0.1 that may apply to you: "Installation issues" on page 4, "Upgrade issues" on page 4, and "Configuration issues" on page 5.
In addition, check at least the following sections of this release note for critical information about Entrust/PKI 6.0 that may apply to you: "Installation issues" on page 14, "Upgrade issues" on page 16, and "Configuration issues" on page 19.

If you are reading these release notes on the Entrust/PKI 6.0.1 CD, these may not be the most recent set. For the most recent notes, check the Customer Support Extranet. The Customer Support Extranet contains online versions of product documentation, an information knowledge base, and problem resolutions. It also provides the ability to submit and track service requests via the Web in a secure manner. You must have an account to access this portal. You can sign up for an account at

`www.entrust.com/xtranet/support/`

Reference information

If you will be using Microsoft® Active Directory® with Entrust/PKI, see also "Entrust/PKI 6.0 and Microsoft interoperability road map" on page 35.

The following white papers and tech notes provide technical information about certain aspects of Entrust/PKI 6.0.1. Note that the white paper *Using Microsoft Active Directory with Entrust/PKI 6.0* has been updated for this release.

- White paper: *Directory Integration: Configuration Guide for Entrust/PKI 6.0*
- White paper: *Entrust Easy Install Requirements for Entrust/PKI 6.0*
- White paper: *Entrust/PKI 6.0 Directory Requirements*
- White paper: *Updating an Existing 8A.x Directory for Entrust/PKI 5.1 and 6.0*
- White paper: *Entrust Directory Schema Requirements for Entrust/PKI 6.0*
- White paper: *Schema Requirements for Entrust/PKI 6.0 with Microsoft Active Directory*
- White paper: *Microsoft Active Directory Integration: Permission Configuration Guide for Entrust/PKI 6.0*
- White paper: *A strategy for migrating from an X.500 Directory to Active Directory with Entrust/PKI 6.0*
- White paper: *Using Microsoft Active Directory with Entrust/PKI 6.0.1*
- White paper: *Entrust/PKI 6.0: Interoperating with Microsoft PKI-enabled applications*
- White paper: *Cross-Domain Client Configuration for Entrust/PKI 6.0 with Microsoft Active Directory*
- Tech note: *Configuring Global Catalogue to support referrals*
- Tech note: *Access Controls configured by Active Directory Configuration*

Note: All white papers and tech notes are posted on the Support Extranet.

How to contact Entrust Technical Support

Entrust offers telephone, e-mail, and online support through the Entrust/Reliance customer care program.

Telephone support

For telephone support, simply call the appropriate number listed in your Customer Resource Kit. The Customer Resource Kit is a package made available to customers after the Entrust/Reliance customer care program has been purchased. You must provide your Unique ID (listed on your Customer Support Extranet account) whenever you call.

E-mail support

E-mail support is offered to provide assistance for non-critical issues. Questions can be sent to

support@entrust.com

Online support

Online support is provided through the Customer Support Extranet. This portal contains online versions of product documentation, an information knowledge base, and problem resolutions. It also provides the ability to submit and track service requests via the Web in a secure manner. You must have an account to access this portal. You can sign up for an account at

www.entrust.com/xtranet/support/

Features modified or removed in this release

- Entrust/PKI 6.0.1 does not support the PeerLogic version 8A2 or 8A3 Directory.
- Entrust/PKI 6.0.1 does not support Secure Electronic Transaction (SET).
- Entrust/PKI 6.0.1 is the last release of Entrust/PKI to support Windows NT.
- Entrust/PKI 6.0.1 is the last release of Entrust/PKI to support PKCS #11 v1 hardware.
- Entrust/PKI 6.0.1 is the last release of Entrust/PKI to support backwards compatibility with Release 4.x of Entrust products.
- Entrust/PKI 6.0.1 is the last release of Entrust/PKI to support the Secure Exchange Protocol (SEP).

Summary of changes and new features

The following is a list of the major changes and additions to Entrust/PKI 6.0.1.

Support for Microsoft Windows 2000 Server SP2 and SRP1

Entrust/PKI 6.0.1 is supported on SP2 and SRP1 of Microsoft Windows 2000 Server. Entrust/PKI 6.0.1 also supports SP2 and SRP1 of Microsoft Windows 2000 Server for the machine hosting Microsoft Active Directory.

New certificate definition file for Identrus

The certificate definition file for Identrus, identrus.certspec, has been updated with three new certificate types to support Identrus OCSP signing, transaction coordinator signing, and OCSP/TC SSL.

Directory support

In Entrust/PKI documentation, "the Directory" can be any Entrust-Ready Directory service that communicates using Lightweight Directory Access Protocol (LDAP). Specifically, "the Directory" means any LDAP-compliant Directory that is identified as Entrust-Ready.

For more information on Entrust-Ready Products, please go to the Entrust-Ready Status Matrix at the following location on the Entrust Support Extranet:

`https://www.entrust.com/support/psic/message.htm`

You must have an account to access this portal. You can sign up for an account at

`www.entrust.com/xtranet/support/`

Logging during upgrade

During upgrade, all actions and results that can be logged are now logged to the installmgr.log file, in the install directory for Entrust/PKI. This file can be used to troubleshoot an upgrade of Entrust/PKI.

Publishing CA certificates with Active Directory

When Active Directory is used, Entrust/PKI now publishes only self-signed root CA certificates to the "CN=Certification Authority,CN=<YourServer>" container. Previously, Entrust/PKI published both link certificates and self-signed root CA certificates to this container.

Installation issues

- If you initially specify that you're using Microsoft Active Directory during installation, but then go back to clear the *Using Microsoft Active Directory* check box, the CA DN still appears in Active Directory format, and is truncated. You will need to enter the CA DN in its proper format (for example, o=Your Company,c=US). You should also verify the format of the default searchbase and of the First Officer DN. If you do not enter the CA DN in the correct format, the Directory Verification Test (DVT) will report an error.
- The Windows installation wizard displays the system requirements for Entrust/PKI 6.0, rather than Entrust/PKI 6.0.1. The supported platforms for Entrust/PKI 6.0.1 are displayed at the beginning of these release notes.
- You cannot install and operate Entrust/PKI 6.0 in a Windows Terminal Server session. You can, however, run Entrust 6.0 clients in a Windows Terminal Server session.

Upgrade issues

- Entrust/PKI 6.0.1 supports the following upgrade paths:

  Release 5.0 to 6.0.1

  Release 5.0.x to 6.0.1

  Release 5.1 to 6.0.1

  Release 5.1.x to 6.0.1

  Release 6.0 to 6.0.1
- If you are running Entrust/PKI 4.x or earlier, you must first upgrade to Entrust/PKI 5.0.x, before further upgrading to Entrust/PKI 6.0.1. Otherwise, you can upgrade directly from Entrust/PKI 5.x to Entrust/PKI 6.0.1. For more information on upgrading from Entrust/PKI 4.x, see Tech Note 4525, "Upgrading from Entrust/PKI 4.x to Release 5.1.1 or Release 6.0", on the Entrust Support Extranet.
- If you've upgraded from Entrust/PKI 5.x to Release 6.0 and want to move your upgraded CA to a clean installation of Entrust/PKI 6.0.x, you must restore from backups. Contact Entrust Support for important information on completing this procedure.
- If you are using protected ACDist with Entrust/PKI 5.x, you should upgrade directly to Release 6.0.1. Do not upgrade to Release 6.0. The database schema version information embedded in the database integrity values was not properly updated for encrypted keys during a 5.x to 6.0 upgrade. As a result, encrypted keys stored in tables that are modified during upgrade were not properly re-encrypted. When upgrading from Release 5.x to 6.0, this was true only for the ACDist key, where protected authcode distribution was enabled. This problem has been fixed and is not an issue when upgrading to Release 6.0.1.
- Before upgrading from Entrust/PKI 5.1 to Entrust/PKI 6.0.1, ensure that all Entrust processes and executables are stopped. Otherwise, the SQL editor will fail and your installation will not be successful.
- If you upgrade from Entrust/PKI 5.x to Entrust/PKI 6.0.x and your upgrade fails, you must revert your system to its pre-upgrade state (that is, revert to Entrust/PKI 5.x). Ensure you revert Informix 9.21 (included in Entrust/PKI 6.0.x) to Informix 7.23 (included in Entrust/PKI 5.x), as database backups from version 7.23 cannot be restored to version 9.21. Once you've reverted your system to its pre-upgrade state, perform the upgrade operation again.

Note: Do not attempt to restore database backups from older versions of Entrust/PKI to newer versions of Entrust/PKI.

Configuration issues

- If you are using cryptographic hardware with Entrust Authority Enrollment Server for VPN 6.0, you must turn FIPS validation off. If you do not, you will receive the following error when you attempt to create an administrative profile using Entrust/RA:

  The following error is returned: (-76) This crypto Hardware device cannot operate in FIPS mode.

  To turn FIPS mode off, open the entrust.ini file and find the [FIPS Mode] section. Set the FIPS= entry as show below:

  ```
  [FIPS Mode]
  FIPS=0
  ```

- On Windows platforms, if you've installed Chrysalis-ITS® Luna® CA3 hardware, the Entrust/PKI configuration utility, "entconfig", may not be able to detect the hardware, due to a caching problem. If you experience this problem, you must exit and restart entconfig so that the cache is flushed and entconfig reads the proper values for the CA3 hardware.
- If you configure the FIPS settings in the entmgr.ini file incorrectly and then attempt to log in to Entrust/Authority Master Control or Entrust Master Control Command Shell (entsh), the login will fail, but the error message displayed refers to the entrust.ini file, rather than the entmgr.ini file. Note that Entrust/PKI, Master Control, and entsh use the FIPS settings in the entmgr.ini file, while Entrust/RA and other clients use the FIPS settings in the entrust.ini file.

Entrust/Authority issues

- When an administrative user updates a user's keys and the CA key is updated before the user has logged in to their profile to complete the key update, the key update will fail. Since the new certificate published to the Directory was signed by the old CA key pair, the client application is unable to verify the new certificate and rejects it. The error that appears in the manager.log file is -11526, "Certificate returned by CA did not verify". To remedy this situation, you must recover the user's profile. To prevent this situation from occurring, ensure that all users complete key update before you update the CA key pair.
- If the latest CA certificate of a root CA is revoked, a new CA certificate is automatically generated, and all revocation lists and policy certificates are reissued and signed with the new CA key. However, since the services are not restarted, other services may continue to use the old CA key for a period of time. To prevent this behavior, the services should be stopped before revoking a CA certificate and restarted after the revocation has been completed.

  If the CA certificate of a root CA is updated, the revocation lists are not immediately reissued. If the previous CA certificate is then revoked, the current RLs will be signed by the revoked CA key, and as a result, certificate validation will fail. You will need to wait until the RLs are automatically reissued (normally less than 24 hours) before certificate

validation will continue normally. Ideally, you should wait until all RLs are signed with the new CA key before revoking the previous CA key.
In either scenario, all existing users will need to be set for key recovery, since their current certificates will no longer be valid.

- After performing a database backup in Entrust/PKI 6.0.1 on Windows, your manager.log file may indicate that the backup operation failed, even if the backup path name did not contain any spaces. Check your mgraudit.log file to confirm the database backup was successful. If the backup was successful, you can safely ignore the error message in the manager.log file.
- In order to re-encrypt your database, the database must be configured with sufficient transaction log space. If sufficient log space is not available, you will receive an error similar to the following:

  2002/06/21 13:04:36 entrust:MGR ,08057:root[-04499 Database failure occurred.] ODBC/Native Error number <-1/-458> : [Informix][Informix ODBC Driver][Informix]Long transaction aborted. : SQL State >> S1000 - dbbase.cpp:1416

  The amount of log space required is dependent on the number of users. For information about increasing transaction log space, contact Entrust Support.

Informix issues

- Do not attempt to install Informix from the setup.exe file located in the Informix folder on the Entrust/PKI 6.0.1 CD. You must install Informix through the main Entrust/Authority installation program.
- The error "Silent execution cannot be executed" when installing Informix on Windows 2000 indicates a problem with spaces in the temporary directory path name. To fix this problem, set your TEMP and TMP local variables to use all short-path type descriptors. For example, change

  `temp=C:\DOCUME~1\`*`your_user_id`*`\Local Settings\Temp`

  to

  `temp=C:\DOCUME~1\`*`your_user_id`*`\Locals~1\Temp`

- You cannot install Informix on a non-primary domain controller (formerly a BDC). If Informix is installed on a domain controller which includes non-primary DC's, the informix user and informix-admin groups are created as domain accounts instead of local accounts (there are no local accounts on DCs). If the machine is a non-primary DC, the account is created on the local machine, but when the service is installed, the validation tries to go to the primary DC. As there hasn't been enough time for the accounts to synchronize with the primary, the service installation fails.

Microsoft Active Directory issues

- If you're using Microsoft Active Directory when Entrust/PKI 6.0.1 is installed on UNIX®, Entrust strongly recommends you use Entrust/RA on a Windows NT or Windows 2000 workstation that is in the same domain as the Active Directory being used by Entrust/PKI. By doing so, you do not need to grant anonymous read access to user,

contact, and computer entries. Using Entrust/RA on a Windows workstation allows you to use NTLM authentication.

To install Entrust/RA on Windows, consult the "Installing Entrust/RA" chapter in *Installing Entrust/PKI 6.0 on Windows*. Once installed, you must add the following entry to the [Directory Connections] section of the entrust.ini file:

```
AuthMethod=WinAuth
```

For more information on using Active Directory with Entrust/PKI, see

- the white paper "Using Microsoft Active Directory with Entrust/PKI 6.0.1", available on the Entrust Support Extranet
- "Installing and configuring Entrust/Authority 6.0.1 on UNIX with Active Directory" in the release notes for Entrust/PKI 6.0.1 on UNIX

Microsoft Interoperability issues

- You cannot perform mutual cross-certification between an Entrust CA and a Microsoft CA. However, you can perform unilateral (offline) cross-certification between an Entrust CA and a Microsoft CA. That is, you can establish one-way trust in which the Entrust CA trusts the Microsoft CA's certificate. Since a Microsoft CA cannot sign a PKCS #10 certificate request, it is not possible to establish mutual cross-certification between an Entrust CA and a Microsoft CA.

Entrust/Timestamp issues

- In the *Entrust/Timestamp 4.0 User Guide*, in the section "To import a TSA certificate", steps 6 and 7 on page 23 are no longer necessary. The semicolons do not appear in the default certificate definition file.

Documentation issues

- The minimum system requirements for Entrust/Authority and Entrust/RA listed in *Installing Entrust/PKI 6.0 on Windows* contain an error. Windows 2000 Advanced Server operating system with Service Pack 1 is listed as a supported operating system for Entrust/Authority 6.0 and Entrust/RA 6.0. Windows 2000 Advanced Server is *not* a supported operating system for Entrust/Authority 6.0 or Entrust/RA 6.0.
- The white paper "Interoperating with Microsoft PKI-enabled applications" describes how to add the sections [CDP] and [CRL] to the entmgr.ini file. However, it does not mention that if you add the section [CDP] with the appropriate settings, the section [CRL], along with its settings, must also be added.
- If you install the Java™ Development Kit on the machine where Entrust/Authority is installed, the table of contents for the Entrust/PKI HTML help may not display properly.
- The white paper "Using Microsoft Active Directory with Entrust/PKI 6.0.1", available on the Entrust Support Extranet, has been updated for Release 6.0.1 of Entrust/PKI.
- The Entrust Master Control Command Shell Quick Reference card (pki_entsh_quick_ref.pdf, found in the "docs" folder on the Entrust/PKI 6.0 CD) has been updated.
- The section "Logging in to the new CA" in the chapter "Maintaining the Certification Authority" of *Using Entrust/PKI 6.0 on Windows* contains an incorrect description of how to use the "MovingDomain=1" flag. The procedure "To edit the entrust.ini file"

states that if the two CAs are cross-certified online, you can add the flag to the user's entrust.ini file to enable automatic key recovery. This is incorrect. If the two CAs are cross-certified (that is, the destination CA can verify the signature on a CMP message signed with a key from the source CA), you can enable automatic key recovery by adding "MovingDomain=1" to the user's entrust.ini file and then having the user log in to their Entrust profile. If the two CAs are not cross-certified, the end user must perform manual key recovery by entering their activation codes (generated when the user was imported). In the case of manual key recovery, the MovingDomain=1 setting must not be included in the entrust.ini. If it is included, you will see an error in the manager.log indicating that the user is not in the correct state.

Localization issues

- By default, the names of Entrust/RA roles and user policies appear in English. If you would like these English attributes to be consistent with the French or Japanese terms, you will need to edit the names. To edit a role or user policy name, left-click the name in the left pane of Entrust/RA and in the right pane of Entrust/RA change from English to either French or Japanese terms used in the localized documentation.

Compatibility issues

For complete details on compatibility between Entrust/PKI 6.0.1 and other Entrust products, see the Entrust Products Platform Support Matrix on the Entrust Support Extranet.

`https://www.entrust.com/support/psic/message.htm`

You must have an account to access this portal. You can sign up for an account at

`www.entrust.com/xtranet/support/`

Problems solved in Entrust/PKI 6.0.1

The following problems have been solved in the Entrust/PKI 6.0.1 release. If any of these problems affect you, you may want to consider upgrading to Entrust/PKI 6.0.1.

Problems / solutions related to all supported platforms
On all platforms, the onlyContainsCACerts flag in the id-ce-issuingDistributionPoint section of the ARL was set to False. This meant that the ARL could contain both user and CA certificates. This problem has been fixed.
The certificate definition file for Identrus, identrus.certspec, was out of date in Entrust/PKI 6.0, so certificates issued did not contain the proper information by default. This file has been updated. In addition, three new certificate types were added to support Identrus OCSP signing, transaction coordinator signing, and OCSP/TC SSL.
If Entrust/PKI was set to issue extra-combined CRLs, and you updated the CA key pair from software to hardware and protected the CA hardware with a password, the previous CA signing keys could not be used to sign the original CRL. This problem has been fixed.

Entrust profiles that were created using the proto-PKIX protocol could not be upgraded to PKIX-CMP format during key update. Entrust User Profiles created in the old proto-PKIX format are now upgraded to the current PKIX-CMP format. PKIX-CMP defines the protocol for managing keys and certificates and supports PKI lifecycle functions.

A new advanced configuration variable, "db set AllowProfileSwitch", enables this upgrade. Log in to Entrust Master Control Command Shell (entsh) and run "db set AllowProfileSwitch 1". Restart the Entrust/Authority services. A user created using the proto-PKIX protocol will now be upgraded to a PKIX-CMP user during key update.

When a PKIX request for a certificate came to Entrust/PKI, the KeyUsage bits in the request (set at a proto-PKIX or PKIX-CMP client) were merged with the keyUsage bits in the certificate type (set in the certificate definition file). The certificate definition file now overrides the client request, and there is no merging of the keyUsage bits.

The CMP Toolkit periodically produces large volumes of certficate requests to Entrust/PKI. A database concurrency issue sometimes occurred when using Entrust/PKI 6.0 with the Informix database 9.21, causing verification certificate requests to fail with error -4499, "Database failure occurred". This issue has been fixed.

When Entrust/PKI 6.0 was operating in Microsoft Compatibility mode with partitioned CRLs, Root CA certificates did not contain pointers to the most recent partitioned CRL file when the CA key was updated. This problem has been fixed.

When CRL distribution points (CDPs) were set in URI format in the entmgr.ini file in Entrust/PKI 6.0, this change was not applied to link certificates (certificates created when the CA key pair is updated). Link certificates now contain CDPs in URI format when this format is set in entmgr.ini.

Entrust/PKI 6.0 could read only the first 10000 bytes of an audit, which could result in a decode error when attempting to query audits larger than 10000 bytes. Entrust/PKI 6.0.1 now reads the first 20 Kb of an audit.

With previous releases of Entrust/PKI, logging in to Entrust with a Luna 2 token could generate PKI error -158, "Miscellaneous crypto key error". Entrust/PKI 6.0.1 now ensures that all keys are Triple-DES-encrypted, so that Luna2 tokens are supported in a Windows 2000 environment.

The database schema version information embedded in the database integrity values was not properly updated for encrypted keys during a 5.x to 6.0 upgrade. As a result, encrypted keys stored in tables that are modified during upgrade were not properly re-encrypted. When upgrading from Release 5.x to 6.0, this was true only for the ACDist key, where protected authcode distribution was enabled. This problem has been fixed and is not an issue when upgrading to Release 6.0.1. If you are using protected ACDist with Entrust/PKI 5.x, you should upgrade directly to Release 6.0.1. Do not upgrade to Release 6.0.

New initialization file settings have been added to control the maximum message size between the administration clients (Entrust/RA and RA Toolkit) and Entrust/Authority.

The following setting in the entmgr.ini file controls the size of the request sent to ASH:

```
[ASH Information]
MaxMessage=<number of bytes>
```

The following setting in the entrust.ini file used by Entrust/RA or by the RA Toolkit controls the size of the response returned from ASH:

```
[ASH Information]
MaxMessage=<number of bytes>
```

If not specified, the default value is 1,000,000 bytes.

The error indicating that a message that exceeds the maximum size has been received is:

```
-8981:Admin API - Bad received message length.
```

When two CAs were mutually cross-certified, and CA2 had a subordinate CA called CA3, moving users from one CA to another could cause Entrust/Authority services to fail. Specifically, Entrust/Authority services would fail on CA1 if the following steps were taken:

- a user was created in CA3
- you updated the CA key pair for CA2
- you waited for CA2 to reissue its revocation lists, signed with the new CA key pair
- you exported the user from CA3
- you imported the user into CA1

This issue has been resolved.

Problems / solutions related to Entrust/PKI in the Windows environment

Upgrading Informix on a Compaq® system that was running Windows NT would fail if you didn't stop the Compaq services (including Compaq Remote Monitor Service, Compaq System Shutdown Service, Insight Agents, Insight Web Agent, and SNMP). This problem has been fixed.

Installing or upgrading Informix would sometimes lead to the system appearing to hang after system restart. Entconfig would be unable to load the database schema, due to filling of the logical logs. Handling of the logical logs has been improved, and error messages for this condition have been clarified. Entrust/PKI now backs up the logical logs before an upgrade, checks their size, and flushes them if necessary.

Upgrading from Entrust/PKI 5.0 to 6.0 would fail if a new client-side setting had been added to the certificate definition file in Release 5.0. Client-side settings added to the certificate definition file no longer cause an upgrade to fail.

Release notes for

Entrust/PKI™ 6.0

Entrust/Authority:
For Microsoft® Windows® 2000 Server with SP1, Windows NT® 4.0 with SP5, SP6, and SP6a

Entrust/RA:
For Microsoft Windows NT 4.0 (SP5, SP6, SP6a), Windows 98, Windows 2000 Professional, and Windows 2000 Server with SP1

Date: June 13, 2001
Release: 6.0 Commercial

Attention: Before you install or upgrade Entrust/PKI or any of its components, check at least the following sections of this release note for critical information that may apply to you: "Installation issues" on page 14, "Upgrade issues" on page 16, and "Configuration issues" on page 19.

If you are reading these release notes on the Entrust/PKI 6.0 CD, these may not be the most recent set. For the most recent notes, see the hard copy that is included with the Entrust/PKI 6.0 software or check the Customer Support Xtranet. The Customer Support Xtranet contains online versions of product documentation, an information knowledge base, and problem resolutions. It also provides the ability to submit and track service requests via the Web in a secure manner. You must have an account to access this portal. You can sign up for an account at

`www.entrust.com/xtranet/support/`

Reference information

If you will be using Microsoft Active Directory with Entrust/PKI, see also "Entrust/PKI 6.0 and Microsoft interoperability road map" on page 35.

The following white papers and tech notes provide technical information about certain aspects of Entrust/PKI 6.0:

- Whitepaper: *Directory Integration: Configuration Guide For Entrust/PKI 6.0*
- Whitepaper: *Entrust Easy Install Requirements For Entrust/PKI 6.0*
- Whitepaper: *Entrust/PKI 6.0 Directory Requirements*
- Whitepaper: *Updating an Existing 8A.x Directory for Entrust/PKI 5.1 and 6.0*
- Whitepaper: *Entrust Directory Schema Requirements For Entrust/PKI 6.0*
- Whitepaper: *Schema Requirements for Entrust/PKI 6.0 with Microsoft Active Directory*
- Whitepaper: *Microsoft Active Directory Integration: Permission Configuration Guide For Entrust/PKI 6.0*
- Whitepaper: *A strategy for migrating from an X.500 Directory to Active Directory with Entrust/PKI 6.0*

- Whitepaper: *Using Microsoft Active Directory with Entrust/PKI 6.0*
- Whitepaper: *Entrust/PKI 6.0: Interoperating with Microsoft PKI-enabled applications*
- Whitepaper: *Cross-Domain Client Configuration for Entrust/PKI 6.0 with Microsoft Active Directory*
- Technote: *Configuring Global Catalogue to support referrals*
- Technote: *Access Controls configured by Active Directory Configuration*

Note: All whitepapers and technotes are posted on the Xtranet.

How to contact Entrust Technical Support

Entrust offers telephone, e-mail, and online support through the Entrust/Reliance customer care program.

Telephone support

For telephone support, simply call the appropriate number listed in your Customer Resource Kit. The Customer Resource Kit is a package made available to customers after the Entrust/Reliance customer care program has been purchased. You must provide your Unique ID (listed on your Customer Support Xtranet account) whenever you call.

E-mail support

E-mail support is offered to provide assistance for non-critical issues. Questions can be sent to

`support@entrust.com`

Online support

Online support is provided through the Customer Support Xtranet. This portal contains online versions of product documentation, an information knowledge base, and problem resolutions. It also provides the ability to submit and track service requests via the Web in a secure manner. You must have an account to access this portal. You can sign up for an account at

`www.entrust.com/xtranet/support/`

Features modified or removed in this release

The functionality of Entrust/PKI 6.0 differs from that of previous releases and several features have been modified or removed. This list describes these changes:

- Entrust/PKI 6.0 does not package an X.500 Directory
- 4.0 bulk processing is no longer supported
- This is the last release of Entrust/PKI that will support the PeerLogic version 8A2 Directory.
- This is the last release of Entrust/PKI that will support PKCS #11 v1 hardware.
- Entrust no longer ships the *Informix Answers Online* CD with Entrust/PKI 6.0. More current information about the Informix database is available at the Informix Web site at http://www.informix.com/documentation/ and http://www.informix.com/answers/english/pids92.htm.

- The What's This? context-sensitive help is not offered in Entrust/PKI 6.0.

Summary of changes and new features

The following is a list of the major changes and additions to Entrust/PKI 6.0.

Microsoft Active Directory support

Entrust/PKI 6.0 provides Microsoft Active Directory support, including:

- A Microsoft Active Directory configuration wizard, including schema and permissions
- Microsoft Windows authentication (NTLM)
- Integration with the Microsoft environment:
  - allows you to publish CA certificates to Authority Information Access (AIA).
  - allows you to publish CA certificates to Certificate Authorities container.
- Enhanced support for CRL Distribution points
- Support for a URI value in AIA so that Microsoft applications can build trust chains while validating certificates.

New Informix database

Entrust/PKI 6.0 uses a more recent version of the Informix database, version 9.21 (where Informix 7.23 was used previously). When you upgrade from Entrust/PKI 5.x to 6.0, Informix 7.23 will be upgraded to Informix 9.21.

Single Key Pair

Entrust/PKI 6.0 allows users to have only one key pair in their profile. This key pair consists of two dual-usage keys: 1) a public key, used for encryption and verification; and 2) a private key, used for both decryption and signing. The Single Key Pair feature is useful for interoperating with third-party S/MIME products that do not use the Entrust dual key pair model.

Enhanced system audit logging capabilities

Entrust/PKI 6.0 includes an hourly audit or "heartbeat" that includes information about your CA and operating system, such as:

- Build version
- Platform
- Hardware specifics
- License Information
- Database Type

Interoperating with Microsoft clients

Entrust/PKI 6.0 interoperates with Microsoft clients. Entrust keys and certificates are available through Microsoft's CryptoAPI interface. This means that many CryptoAPI-aware applications (such as Microsoft Outlook, Internet Explorer, and Microsoft Word) can use Entrust through their own built-in PKI-aware capabilities. This allows you to deploy and automatically leverage Entrust's key and certificate management features, in addition to

using the advanced Windows 2000 management capabilities built into Microsoft Active Directory.

CA key rollover interoperation with Microsoft clients

Entrust/PKI 6.0 allows a CA key rollover to occur while supporting Microsoft clients. As it does so, Entrust/PKI 6.0 disallows revocation list substitution attacks that might otherwise compromise the security for Entrust, Microsoft, and other clients.

Elliptic Curve DSA

Entrust/PKI 6.0 offers Elliptic Curve DSA as an additional algorithm choice for your CA signing key.

Support for Advanced Encryption Standard (AES)

Entrust/PKI 6.0 now provides support for the Advanced Encryption Standard (AES) algorithm for encryption of the Entrust/Authority database.

Longer CA key lifetimes

Entrust/PKI 6.0 allows long lifetimes for the CA keys, up to 35 years or until 2037, whichever is less.

Enhanced Database Protection

Entrust/PKI 6.0 provides enhanced database security by allowing database passwords to be protected with a separate CA hardware device module. A CA hardware device is required to use this feature.

HTML help linked to Entrust/RA

Entrust/PKI 6.0 includes an HTML version of "Administering Entrust/PKI 6.0 on Windows" and "Using Entrust/PKI 6.0 on Windows". This HTML help is available in Entrust/RA.

HTML help is not available with Entrust/Authority Master Control.

Browser requirements: You require at least Netscape 4.72 or Internet Explorer 5.0 to run the HTML help.

If you are running Entrust/PKI 6.0 for DOCSIS

Check the Entrust Support Xtranet for a related tech note.

Installation issues

- If you plan to install Entrust/PKI 6.0 on Windows 2000 for use with Microsoft Active Directory, make sure that you install MS Windows 2000 SP1 on the machine hosting the Authority component of Entrust/PKI.
- If you're using Microsoft Active Directory, when installing Entrust/PKI 6.0 on the Windows 2000 platform, you must log in to the machine that will host Entrust/PKI with the exact domain account name (including case) you entered when configuring Active

Directory. To use Entrust/PKI after installation, you must continue to log in to the machine with the same case-sensitive name. Also, ensure the domain account you use to log in is a member of the local Administrator's group for the machine that will host Informix and Entrust/Authority. Membership in the local Administrator's group grants the domain account permissions for installing Informix and Entrust/Authority, and for setting up and running the Entrust/Authority service.

- If you're using Microsoft Active Directory, and if you log in to the Windows server using a Windows domain account other than the account you created using the Entrust Microsoft Active Directory Configuration wizard, ensure this domain account is configured with the appropriate permissions to use Microsoft Active Directory. These permissions are required for both Informix and Entrust/Authority.
- When you configure Entrust/PKI 6.0, make sure you enter the CA's distinguished name correctly (the first time) in the CA Distinguished Name and Password dialog box. If you go back and change the CA DN, the initial searchbase value is not updated accordingly (even should you change the value in the Advanced Directory Attributes dialog box). To solve this problem, you must create a new searchbase after configuration using Entrust/RA. The new searchbase will have the correct CA DN.
- When you install Entrust/PKI 6.0, the installation program checks connectivity and read/write access to the Directory. Under normal circumstances the Directory Verification Tool (DVT) should run to completion in approximately one minute. If, however, the Directory fails to respond to a Directory operation, the DVT may take up to six minutes to time out of the request and terminate.
- You cannot install and operate Entrust/PKI 6.0 on a Windows NT Server, Terminal Edition. You can, however, run Entrust 6.0 clients on a Windows NT Server, Terminal Edition.
- When you install Entrust/PKI 6.0, Entrust highly recommends that you do not perform the install with a user account (that is, the user account the installer is logged in as) that contains an upper-case character. If the user account name includes an upper-case character, you can't create new or view older reports.
- If you have also purchased Entrust Authority Roaming Server, note that the Roaming Server software should be installed on a dedicated machine that is physically restricted except to the most trusted administrators. Do not put Entrust/PKI and Roaming Server on the same machine. For more information refer to the user documentation included with the Roaming Server product.

Changes to Windows installation guide

- In Step 7 of the procedure "To configure Entrust/Authority" in the "Installing and configuring Entrust/Authority" chapter, if you clear *Using Microsoft Active Directory*, go to Step 9.
- The procedure "To add new client-side settings to the certificate definitions file" in the "Upgrading to Entrust/PKI 6.0" chapter is no longer applicable. The initial.certspec changes are automatically applied during an upgrade.

  You need only manually upgrade the master.certspec file when a conflict occurs (that is, some of the new entries have already been added to the master.certspec). In this instance, the master.certspec is not upgraded.

- After Step 12 in the procedure "To install Entrust/Authority" in the "Installing and configuring Entrust/Authority" chapter, you may be asked to restart your computer. If you choose to restart your computer, remove any floppy disks and bootable CDs from your computer's drives. After your computer restarts, log in using the same account that was used to initiate the Entrust/Authority installation. Now you're ready to configure Entrust/Authority. Go to the "Configuring Entrust/Authority" section in the "Installing and configuring Entrust/Authority" chapter.

Checking for mirrored dbspaces

This note applies to fresh Entrust/PKI 6.0 installations only. If you are upgrading from a previous release of Entrust/PKI to Entrust/PKI 6.0, this note does not apply to you.

1. After you have installed and configured Informix, but before you install Entrust/PKI 6.0, you'll need to check for mirrored dbspaces by running the following query from a DOS window:

   ```
   C:\>onstat -d
   ```

2. If there is no rootdbs_mirr.000 file, then mirroring is not enabled and this note does not apply to you. Proceed with installing Entrust/PKI 6.0.
3. In the unlikely event that the result of the onstat command finds a file called rootdbs_mirr.000, note the location and size of the data files (chunks), and proceed to the Entrust Support Extranet for a related tech note *before* you install and configure Entrust/PKI 6.0. The tech note number is 3468, “How to remove mirrored dbspaces”.

Upgrade issues

Upgrade paths

If you are running Entrust/PKI 4.x or earlier, you must first upgrade to Entrust/PKI 5.0.x, before further upgrading to Entrust/PKI 6.0. Otherwise, you can upgrade directly from Entrust/PKI 5.x to Entrust/PKI 6.0.

Stop Compaq services before upgrading

Before you upgrade Informix on a Compaq system that’s running Windows NT, you must stop the Compaq services, otherwise the upgrade will fail. These services include Compaq Remote Monitor Service, Compaq System Shutdown Service, Insight Agents, Insight Web Agent, and SNMP.

Migrating to Entrust/PKI 6.0 with Microsoft Active Directory

Please note that these upgrades apply to Entrust/PKI 6.0 when using an X.500 Directory. There is no upgrade path using Microsoft Active Directory. If you are migrating to Entrust/PKI using Microsoft Active Directory, see the white paper entitled *Migration from X.500 to Active Directory*, found on the Entrust Support Extranet.

Upgrading from Preview to Commercial

You cannot upgrade from Entrust/PKI 6.0 Preview to Entrust/PKI 6.0 Commercial. Entrust does not support this upgrade path. You will need to uninstall the Preview product before you install the Commercial version.

Manually upgrading the master.certspec file after an upgrade

When you upgrade from Entrust/PKI 5.1 to Entrust/PKI 6.0, the master.certspec file is automatically updated; however, if you receive a message indicating that the new client-side settings were not added to the master.certspec file, you must manually upgrade the master.certspec. (Note, if you are upgrading from Entrust/PKI 5.0, you may also need to merge the contents of certspec_changes.v51 into the master.certspec file.)

To do so, you must copy the information from the certspec_changes.v6 file into the master.certspec file. In certspec_changes.v6 there are two sections marked [update:<section name>]. These sections contain existing entries that must be modified. Within these sections, the entries are "old:<entry name>=<old value>" and "new:<entry name>=<new value>". These entries already exist in the old master.certspec; replace the old values should be replaced with the new values.

Using attribute certificates

If you plan to use attribute certificates, consult the white paper entitled *Updating an Existing 8A.x Directory for Entrust/PKI 5.1 and 6.0*, found on the Entrust Support Extranet.

Moving users across CAs

When moving users from one CA to another, imported users on the destination CA are placed in Import Key Recovery state. Key recovery is completed automatically the next time a user logs in. However, key recovery is not completed automatically when a user logs into Entrust Desktop Solutions 5.0.2. If using Entrust Desktop Solutions 5.0.2, the user will have to obtain activation codes from their Administrator and complete the key recovery manually.

Improving search speed after an upgrade from Entrust/PKI 5.0.x

The following entmgr.ini file setting may help improve the speed at which you can search on the distinguished name (DN) field, if

- you are upgrading from Entrust/PKI 5.0 to Entrust/PKI 6.0
- you have a large database
- you have a large amount of free disk space (about 200 MBytes per 1 million users)

```
[login]
userSearchExplicitWildcardPrefix=true
```

If you have upgraded to 6.0 from version 5.0 and you want to take advantage of the userSearchExplicitWildcardPrefix setting to improve search speed, add temporary disk space to the database and add the index to the database as described in the procedures below. Note that this index is only useful in conjunction with the .ini file setting.

To add temporary disk space to the database

1. Verify that you have enough disk space (approximately 200 MBytes per 1 million users).
2. Add the temporary space to the database. At the DOS prompt, enter:

   onspaces -c -d tmpdbs2 -t -p *<path>* **-o 0 -s** *<size>*

   where *path* is a filename (path must refer to a fully-qualified path to an existing file, which should be 0 bytes. One can be created by first executing "type NUL > <PATH_TO_FILENAME>)

   where *size* is the number of Kbytes you want to add
3. Using a text editor, add `tmpdbs2` after `DBSPACETMP` in the informix\etc\onconfig file; for example:

   ```
   DBSPACETMP tmpdbs2
   ```
4. Open the Services control panel and stop and start Informix IDS 2000 - entrust_nt.

To add the index to the database

1. Shut down the Entrust/Authority service for your CA.
2. Change the directory to \informix and enter the following command:

   `dbaccess <dbname> dbv51upg_manual.sql`

   This command may take as long as one hour per 1 million users.

To remove the temporary disk space

1. If you decide to remove the temporary space later, enter:

   onspaces -d tmpdbs2
2. Using a text editor, remove "tmpdbs2" that appears after DBSPACETEMP in the informix\etc\onconfig file.
3. Stop and restart Informix.
4. Restart the Entrust/Authority service for your CA.

Interoperating with Microsoft PKI-enabled applications

If you are upgrading from Entrust/PKI 5.1 to Entrust/PKI 6.0 and you want to interoperate with Microsoft CryptoAPI-enabled applications, you must first set the CA private key usage period to 100%. User certificate lifetimes can extend up to, but not past, the lifetime of the CA public key (CA certificate).

Note: The CA private key usage period refers to the lifetime of the CA private key which is defined as a percentage of the CA certificate lifetime. Entrust/PKI 6.0 will only use the CA private key up to its lifetime. If the private key usage period is less than the lifetime of the CA certificate, Entrust/PKI 6.0 will stop issuing the revocation list required by Microsoft. This means that after the CA private key expires, Microsoft client revocation checking will fail for certificates whose life extends beyond the private key usage period.

For more details on interoperating with Microsoft PKI-enabled applications, see the white paper *Entrust/PKI 6.0: Interoperating with Microsoft PKI-enabled applications*, available on the Entrust Support Extranet.

Configuration issues

- Release 6.0 Entrust products are not fully supported by the Luna2 hardware token with software version 3.4 (or earlier) and firmware version 1.12 (or earlier). The Luna2 hardware tokens do not correctly accept 2048-bit RSA decryption private keys. If you configure a Luna2 user with those versions to have 2048-bit RSA encryption keys, the user creation process will fail.
  Check the Chrysalis web site (http://www.chrysalis-its.com) for more information about more recent versions of software for their hardware token products.
- If you choose to interoperate with Microsoft CryptoAPI-enabled applications, Entrust/PKI 6.0 will be automatically configured as follows:
  - the CA private key usage period will be set to 100%
  - the MSCompatibility Advanced Setting in the entmgr.ini file will be enabled
  For more information about interoperating with Microsoft clients, see the white paper entitled *Entrust/PKI 6.0: Interoperating with Microsoft PKI-enabled applications*, available on the Entrust Support Extranet.

Entrust/Authority issues

- Do not create backup files of the form entmgr.ini<uniqueterm> in the manager directory. Entrust/PKI 6.0 automatically detects these files and will restore the entmgr.ini file. This will undo whatever changes you have made to this file. For example, if you create a backup copy of the entmgr.ini file called entmgr.ini.old or entmgr.ini.bak or entmgr.ini.20000102 and then changed the entmgr.ini file, when you run the PKI, it will detect the backup copy and copy its contents back to the entmgr.ini file. This will remove all the changes made to the modified .ini file. To solve this problem, do not store the backup copy in the authdata\manager directory.
- The values for the ENTTCPBACKLOG and ENTTCPLINGER environment variables are configurable. These environment variables control the TCP backlog and TCP socket lingering connections that allow data to be transmitted. The default value for ENTTCPBACKLOG is 5 and the default value for ENTTCPLINGER is 60 seconds. To turn off the ENTTCPLINGER variable, type a value of -1.
- If you attempt to log in to Entrust/Authority Master Control before you activate the Chrysalis Luna CA hardware for Entrust, you are asked to reselect the hardware device. To correct this problem, exit Entrust/Authority Master Control and activate the Luna CA hardware for Entrust using the Luna Enabler application. Then log in to Entrust/Authority Master Control and, if requested to do so, reselect the hardware device.
- You can change end-user password rules by editing the master.certpec file and using a DER-encoded value. When you do so, the password rule changes will not take effect immediately. Restart the Entrust/Authority services to affect the password rule changes.
- If you store the CA keys on an nCipher hardware device, do not remove the token during operation. If you remove the card during an administrative operation the CPU usage on the machine will rise to 100% and will hang the machine. Replacing the token will not cause the machine to resume operation and you must reboot the machine to continue.
- If you use hardware-based database protection, the database restore operation may fail on the last step when you enter the Master User password. Solution: Log in to Entrust

Master Control Command Shell and run the following command after you are prompted to re-enable hardware-based database protection:

```
ca resynch-next-cert-serial
```

- You cannot issue the default Web certificate type if the key in the certificate is an elliptic curve (ECDSA) key. The default Web certificate type includes the keyUsage extension which indicates that the key may be used for signing and encryption operations (digitalSignature and keyEncipherment). However, ECDSA keys can only be used for signing. Solution: Create a new certificate type with keyUsage of digitalSignature. For more information, see "Creating and modifying a user certificate type" in *Administering Entrust/PKI 6.0 on Windows*.
- If you are using Entrust/PKI 6.0 with Microsoft Active Directory and you choose a long CA DN name, the name may be truncated in the Entrust/Authority Master Control window.
- Entrust recommends that you contact Entrust Support before you exceed the user limit allowed by your CA license. If you exceed the user limit, you will be locked out of the CA and you will have to contact Entrust Support for a new license code.
  Note that Entrust/PKI 6.0 includes a new entmgr.ini setting (entLicenseThreshold) that allows you to raise an alarm when the percentage of licenses used barrier is reached.
- If you receive a "General Entrust Error" when you start the services, it may be due to the services taking longer to start than Entrust/Authority Master Control or Entrust Master Control Command Shell expects. If this problem persists, check the manager logs for further information.
- Occasionally there may be problems shutting down the Entrust services when you re-encrypt the database. If you intend to re-encrypt the database, it is recommended that you shut down the Entrust services before doing so.
- You may receive the following message when you add a user and include a serial number where the uniqueness of the serial number cannot be determined:
  - (6267) No such object <Name Error: No Such Object>
  This may occur when a searchbase destination in your CA can't be accessed. Confirm that your CA can communicate with the Directory(s) referenced by your CA's searchbases' DNs, then resolve any Directory connection, configuration and permission problems or remove the offending searchbase(s) from your CA.
- You cannot change the nCipher token from "password enabled" to "password disabled". If you do so, you will receive an error message the next time you try to log in to Entrust/Authority Master Control. Solution: change the token back to "password enabled."
- Do not use Informix backup commands (such as ontape) unless you have disabled Entrust database backups. Using Informix backup commands will corrupt the Entrust database backup file set. To disable Entrust database backups, change the disableDbBackup setting in the entmgr.ini file to true.
- Do not set a certificate extension to "critical" and attempt to initialize a user using a client application (such as Entrust/RA or Entrust/Entelligence). If you do so, the user initialization will fail and you will receive an error message.
  For example, if you use Entrust/RA and Entrust Entelligence to initialize the user, you may receive the following error message (or a message similar to this):

```
"(-11526) Certificate returned by CA did not verify"
```

To avoid this, the certificate extension should be set to "non critical."

For information about setting the criticality of certificate extensions, see "Editing Certificate Extensions" in *Administering Entrust/PKI 6.0 on Windows*.

- If you move a user from one CA to another CA (and these two CAs share one Directory) and keep the same DN for the user, make sure you finish the export operation before allowing the user to log in. Otherwise, the following error message will appear when the user logs in:

  ```
  (-1048) Your certificates are no longer valid. Contact an administrator.
  ```

  For more details, see "Completing the user export" in *Administering Entrust/PKI 6.0 on Windows*.
- If you select "Rename existing Directory entry" when you change a user's DN in the Change DN dialog box, you may attempt to add mandatory attributes that already exist in the Directory for the entry. If so, some Directories may return unexpected errors and the Change DN may fail. If this happens, re-enter the Change DN information and choose "Keep old entry in the Directory". If this option isn't feasible, you can use your own Directory tools to change the DN and reassign the new DN to your user.

Informix issues

Required Informix database maintenance procedure after activating first 1000 users

When you use Informix 9.21, performance degradation occurs after 1000 users are activated. As the database grows, the initial query optimiser is no longer appropriate and needs to be updated with new statistics. To restore performance, complete the following maintenance procedure after the first 1000 users are activated.

Note: It is not necessary to perform this procedure after upgrading from version 5.x. This procedure applies only to first-time installations of Entrust/PKI 6.0.

1 At the prompt, enter

```
dbaccess <database_name> -
```

For example:

```
dbaccess entrustv6 -
```

2 The following appears on screen:

```
Database selected.
```

3 At the prompt type:

```
update statistics high;
```

4 When the update is complete, the following appears on screen:

```
Statistics updated.
```

5 When the prompt returns, exit dbaccess by pressing Ctrl-C.

This procedure will take a few minutes for a database of around 1000 users and around half an hour for 100,000 users. It is recommended the procedure be done while the database is still small. It is not necessary to repeat the procedure after more users are activated. After the procedure completes, stop and restart the services and exit Entrust Master Control Command Shell or Entrust/Authority Master Control if it was running.

Other important Informix issues

- Informix cannot handle a backup with a filename longer than 68 characters or a filename that contains spaces. The database backup filename usually consists of the configured backup directory and the backup name (42 characters), for example: \mgrbk20000810170856\Database\ifmxbkup.bak

  Because this database backup filename uses 42 characters, the configured backup path can include up to 26 additional characters.
- You cannot install Informix on a non-primary domain controller (formerly a BDC).

Directory issues

- When chaining DSAs, if the second DSA uses a context prefix that's subordinate to the context prefix in the first DSA, use a subordinate-reference, not a cross-reference. For example, if DSA 1 has a context prefix of "o=Your Company,c=US" and DSA 2 has a context prefix of "ou=Sales,o=Your Company,c=US", the subordinate-reference should be used to chain from DSA 1 to DSA 2. If you try to use a cross-reference instead of a subordinate-reference, the DSA will respond with an error (for example, "XDS: Service Error: Unwilling to Perform"). After creating the subordinate reference from DSA 1 (o=Your Company,c=US), a superior reference needs to be created from DSA 2 (ou=Sales,o=Your Company,c=US) to DSA 1 (o=Your Company,c=US). If there's no relationship between the two context prefixes (or if neither context prefix is subordinate to the other), then cross-references should be used for both DSAs.
- After installing the PeerLogic i500 Directory, Entrust recommends that you either delete or secure the following files from the DSA database folder: du.000, du.001, odsgen, and odsegen. These log files contain the Directory Access passwords for the i500 Directory Manager, CA, and Entrust Directory Administrator.
- The PeerLogic i500 Directory supports two formats for CA-signed attributes (this includes the userCertificate, caCertificate, certificateRevocationList, attributeCertificate, authorityRevocationList, and crossCertificatePair attributes). The first format is "ASCII", where each byte is represented as a pair of hexadecimal ASCII characters (for example, {ASN}308209A4). This is configured by specifying the LDAP syntax in the oidtable.at file as "unknown". The second format is "binary", where each byte is represented without modification; the original DER binary encoding is transmitted. This is configured by specifying the LDAP syntax in the oidtable.at file as "jpeg:file". The binary representation can also be configured with the LDAP syntax "Binary" with version 8A of the PeerLogic i500 Directory. For the purposes of chaining and replication (X.500 protocol interoperability), it's possible for two i500 DSAs that are configured as "unknown" and/or "Binary" to interoperate without problems. However, it's not possible for an i500 DSA configured as "jpeg:file" to interoperate with an i500 DSA configured as either "unknown" or "Binary". An i500 DSA configured as "jpeg:file" may also have X.500 protocol interoperability problems with third-party X.500 products.

- During the installation of the PeerLogic i500 Directory, attribute names are case sensitive. For example, you must use "ou=" for organizational unit, not "OU=".
- If you are using version 8A of the PeerLogic i500 Directory and check the schema using iCon, iCon may report a number of inconsistencies in the Entrust schema. This is expected, do not try to correct these consistencies using iCon, as loss or corruption of data may result.
- If you are using version 8A.2 of the PeerLogic i500 Directory, and check the schema using iCon, you will need to enable iCon and register the DSA to ensure that the DSA starts automatically on reboot.
- If you're using the LDAP version 3 server with version 8A.2 of the PeerLogic i500 Directory (included with Entrust/PKI 5.0.x and 5.1), the leading and trailing spaces of attributes within a DN aren't properly rendered with respect to RFC 2253. These entries will appear without the leading and trailing spaces. For example, the DN

  cn=" John Smith ", o=Your Company, c=US

  is formatted by the LDAP v3 server as

  cn=John Smith, o=Your Company, c=US
- If you have been operating the Latin1 LDAP version 2 (odsldap) server with i500 8A, there may have been compatibility problems with LDAP version 3. The LDAP version 2 server performs character set translation on ASN.1 encoded objects such as certificates and CRLs. This causes the character set information to be altered when the data is transmitted in LDAP version 3. This is only a problem if non-ASCII data is being used. In order to prevent this, the dsaptailor file contains the following entry:

  ```
  latin-1_no_conversion userCertificate cACertificate authorityRevocationList
  certificateRevocationList crossCertificatePair deltaRevocationList
  attributeCertificate attributeCertificateRevocationList confKeyInfo
  aACertificate crossPrivilegeCertificate attributeAuthorityRevocationList
  attributeDescriptorCertificate messageDigest countersignature
  userSMIMECertificate userPKCS12 entrustAttributeCertificate
  attributeCertificateAttribute
  ```

  Note: Each item in the list above may be configured in the LDAP schema.

  If this setting does not appear in your dsaptailor file, and non-ASCII data has been used, please contact Entrust Support to correct any issues that may emerge.
- There is an error in the schema configuration in the Easy Install package. The object class entry "dnQualifiedUser" should be changed to "entrustDNQualifierUser" in the objectclasses.cfg file.
- Entrust/PKI 6.0 uses two attributes with similar names for different purposes: "attributeCertificate" for the backwards compatibility policy publishing, and "attributeCertificateAttribute" for end user attribute certificates. Entrust/PKI 6.0 uses the LDAP "attributeCertificate" attribute included with the entrustCA object class in the CA entry to publish security policies for backwards compatibility with Entrust 4.0 or earlier clients. As of Entrust/PKI 6.0, the Attribute Authority feature uses a different attribute named "attributeCertificateAttribute" (defined in X.509 2000 ed.), included with the pmiUser object class, to issue end-user Attribute Certificates.
- Directory communications between the two CAs must be established when you cross-certify two CAs. This is usually achieved by chaining the two Directory products. If chaining isn't possible, you can enable LDAPv3 referrals (by which the clients can access

the remote Directory). Entrust software does not enable referral processing by default; so if referral processing is necessary, the entrust.ini files must be modified. In this situation, Entrust recommends that you configure the clients for referral processing by distributing the required setting in the entrust.ini file as part of the client install package. The required entrust.ini file setting is as follows:

```
[Directory Connection Settings]
ReferralDepthLimit=2
```

Note: The assigned value must be a non-zero setting.

LDAP version 2 backwards compatibility

If LDAP version 2 and LDAP version 3 is used to access the same Directory, it is important to determine if backwards compatibility is properly supported by the Directory. An example of such a configuration would be if Entrust/PKI 4.x or earlier versions is used together with Entrust/PKI 6.0 where the PKI is running in LDAP version 3 mode (earlier Entrust products only support LDAP version 2). The following is a list of features which may cause compatibility problems:

Proper support for the “;binary” attribute option

LDAP version 3 uses the ;binary option to access userCertificate, caCertificate, authorityRevocationList, certificateRevocationList, crossCertificatePair, attributeCertificateAttribute, and attributeCertificate. LDAP version 2 does not include the use of attribute options, however some Directory products require the use of “;binary” in order to access attributes in LDAP version 2. If the Directory requires the use of ";binary" in LDAPv2 and you are using Entrust products in LDAPv2 (or you are upgrading to use LDAPv3) a configuration may be available to allow compatibility. Contact Entrust Support for more information.

RFC2253 DN formatting

RFC2253 defines how DNs that are generated by LDAP version 3 applications must be formatted. The allowed format is a subset of the available formats previously defined in RFC1779. For example, RFC1779 allows the quoted format as well as the escaped format as shown below

```
cn=”John Smith + E12”, o=Your Company Inc., c=US (allowed by RFC1779 / LDAP
version 2)
cn=John Smith \+ E12,o=Your Company,c=US (mandated by RFC2253 / LDAP version 3)
```

Release 4.x and earlier versions of Entrust/PKI and client applications don’t support the escaped format which uses the slash “\” character to escape special characters. This problem is only manifested if the following special characters are used in attribute values: , = + < > # ; \

Character set encoding

If support for both LDAPv3 and LDAPv2 is detected, the Directory Verification Tool (DVT) will test the character set used by your Directory in LDAPv2 to determine if you may encounter problems. If the DVT reports an error for the Language Encoding Test and you

intend to use non-ASCII characters in DNs or other string attributes, contact Entrust Support for more information on how to configure your Directory for Latin-1.

Password restrictions

In order to maximize interoperability among products, it is important to restrict Directory passwords to the 7-bit ASCII character set. This will affect the Directory passwords for the CA and Entrust Directory Administrator as well as any Directory passwords assigned to Entrust users. For PKI installations which include the i500 Directory, this will also affect the i500 Directory Manager password. This will not affect the EPF passwords created during user initialization.

If you are using the i500 Directory, you cannot use the following characters in Directory passwords:

Character Symbol	ASCII Hexadecimal Value
#	23
$	24
^	5e
`	60
~	7e
/	2f
|	7c
\	5c

Microsoft Active Directory issues

- If you are using Active Directory, use the "Manage this computer" tool to add the Entrust CA Windows account to the Administrators group for server #2. If you do not set up this account with local administrator privileges, the installer will not be able to establish to Entrust/PKI as a service. Once you have set up the appropriate privileges, log in to server # 2 and run the installation as that user, for example, if you created your Entrust CA Windows account in entADConfig with the name EntrustCA, you will install Entrust/PKI while logged in as EntrustCA.
- When you run entADConfig, you can open a log viewer to review the changes made to your Directory schema. If you run entADConfig several times (for example, if you have received an error) the log file becomes quite large and the log text may be truncated. Open the file directly to view the log.
- Using Entrust/PKI 6.0 with Microsoft Active Directory, the Change DN feature is unavailable. If you attempt to change a user's DN using the right-click menu you will receive an undefined templates error. You must first change the user's DN in Active Directory using Microsoft tools, and then assign the new DN to the user in Entrust/RA

or with bulk scripts. To assign a new DN in Entrust/RA, right-click the user and click Assign new DN in the pop-up menu.

- By default, CRL checking is not enabled in Microsoft Outlook Express. You must use Entrust Express for revocation checking using Outlook 2000. Note: These issues do not affect Outlook Express.
- If you set up two domains (Domain 1 and Domain 2) in a single Microsoft Active Directory Forest, each with a unique CA and Microsoft Exchange Server, the default email address used by the Domain 2 Entrust/PKI uses the suffix derived from Domain 1. This results in a mismatch between the email address included in a Domain 2 user's certificate and that user's email address found in the Exchange Server database, and Outlook Express will not allow the certificates to be used for email encryption. To solve this problem, manually edit the email address included in the certificate of the Domain 2 user to match the email address in the Exchange Server database. Note: This problem does not affect Microsoft Outlook 2000.
- If you install Service Pack 1 for Microsoft Active Directory, add the following setting to all of the entrust.ini files on your system:

  ```
  PreventFilterOptions=1
  ```

- If the machine hosting Active Directory has Service Pack 1 installed, you must add the following setting to the entrust.ini file for administrative users:

  ```
  [Directory Connection Settings]
  LDAPModifyOperation=Replace
  ```

  This entry determines whether an LDAP "modify" operation is performed as a replacement or performed as two steps (a deletion and an addition). The LDAPModifyOperation=Replace entry is required in the entrust.ini file for administrative users because of a problem mapping LDAP operations to ADSI in Service Pack 1 of Active Directory. Setting this entry to Replace configures Entrust/Authority to format all of its LDAP modify operations using "Replace" instead of "AddAndDelete".

Microsoft Interoperability issues

- In Entrust/PKI 6.0, you cannot establish a trust relationship between two CAs where the Entrust CA is subordinate to a Microsoft CA. You can, however, establish a trust relationship where the Microsoft CA is subordinate to an Entrust CA. When a Microsoft CA issues a certificate for a subordinate CA, it does not include the full DN in the subject field (that is, it ignores DC= RDNs in the PKCS #10 request).
- You cannot cross-certify a CA running Microsoft Active Directory with a CA running a Directory that does not support referrals.

Entrust/RA issues

- Users of Entrust/RA 6.0 who are also using Microsoft Active Directory will note differences in the Entrust/RA graphical user interface from that used with an X.500 directory. For example, you cannot add new users through Entrust/RA 6.0 when using Microsoft Active Directory. For a complete list of the GUI modifications, please see the *Using Microsoft Active Directory with Entrust/PKI* white paper, available on the Entrust Support Extranet.

- The UTCTime data format isn't supported when used as a DateTime variable type in the certificate definitions file. UTCTime uses a two-digit year format (for example, "9701020001Z") and GeneralizedTime uses a four digit format (for example, 199701029991Z).
- In Entrust/PKI 5.0, the session credentials that Entrust/RA used to communicate with the Entrust/Authority service were valid for 1 week. In Entrust/PKI 6.0, the session lifetime in seconds is set using the DefaultCredentials_time_req setting in the [Entrust Settings] section of the entrust.ini file. After installing Entrust software, this is typically set to 43200, which is 12 hours. If the setting is missing or set to 0, an indefinite session is used.
- When a Security Officer or Administrator using a Luna2 token logs in and both key pairs update simultaneously as a result of a forced key update, one of the following errors may occur when they attempt to do an operation that requires authorization:

  ```
  Cryptoki device not found
  ```
  or
  ```
  Profile not found on Cryptoki device
  ```

  Restart Entrust/RA to resolve this problem.
- Entrust/RA includes a new check box called *Retain old DN values in the entry*. If you want to remove the old DN values when you change a user's DN, clear this check box. However, clearing this option may occasionally cause the Change DN operation to fail. If this happens you will have to check the option, perform the Change DN operation and manually remove the values afterwards.
  A failure may occur, for example, when removing a serialNumber from the DN; for example, changing the DN from "cn=Joe Smith + serialNumber=123,o=Entrust,c=ca" to "cn=Joe Smith,o=Entrust,c=ca". In this case the Directory will likely return an error ("objectClassViolation") if you clear *Retain old DN values* in the entry check box. This happens because the entry contains the object class uniquelyIdentifiedUser which has serialNumber as a mandatory attribute. If the serialNumber attribute is removed without also removing the object class uniquelyIdentifiedUser, an object class violation will result.
- In order to create a user's profile on a Luna 2 token using Entrust/RA, the token reader must be able to accept two tokens at once. To ensure successful profile creation, the administrator's token must be inserted in slot 1 and the token where the profile is to be created must be inserted in slot 0. Note that if the administrator and user tokens are reversed, the user will be created, but their profile will not. In this case, the administrator will be presented with the user's activation codes.
- When adding a user entry to the Directory, or changing the DN of a user, Entrust/RA searches all searchbases to verify the uniqueness of any values specified for attributes, such as serialNumber, which are marked as unique in the user templates. If Entrust/RA is unable to search all searchbases to verify that a value is unique, the user operation will fail. This may occur if a searchbase is invalid or unavailable.

  One solution is to correct the problem with the searchbase. Alternatively, the uniqueness check can be prevented by marking all attributes as non-unique in the user templates.

  For example, the default Person template contains one attribute that is marked as unique, serialNumber. To configure the serialNumber attribute in the Person template as

a non-unique attribute, change the value for the third numeric field in the definition from 1 to 0. For example, the line for the serialNumber attribute in the Person template should read as follows:

```
2=Serial Number,serialNumber,0,0,0,uniquelyIdentifiedUser
```

- Non-administrative Entrust users in the "export hold" state may log in using their Entrust profiles and work with Entrust applications. The exception is Entrust/RA. A user in this state cannot log in and use Entrust/RA.
- If you are an administrator and plan to store your Entrust profile (.epf file) on a token, make sure that your installation of Entrust/RA and related entrust.ini file includes the Cryptoki entries. If the entrust.ini file does not include these entries, Entrust/RA will not detect the token reader hardware. Note: Cryptoki entries may also exist in the ethardware.ini file. This file allows you to specify multiple hardware devices.
- When running large bulk files, memory usage will grow until either the bulk process is completed and you close the console window or you click the *Log* button to close the console window. If you don't need to monitor the output, close the log window to avoid using excessive memory.
- You will receive the following error when you attempt to create a new policy and enter the date in yyyymmddhhmmss (for example, 19990505120521):

  - ***(-8175) Extension/Attribute value parameter is invalid.

  Instead, enter the date value in yyyymmddhhmm with no seconds (for example, 199905051205).

Entrust/Timestamp issues

Locating the enttimestamp.ini file

If you're installing Entrust/Timestamp 4.0 SP1 on a computer where Entrust/Authority 6.0 is installed, the file "enttimestamp.ini" is placed in the Windows directory (for instance, c:\winnt). You must copy "enttimestamp.ini" to the directory containing the Entrust/PKI initialization file (that is, entmgr.ini). By default, entmgr.ini resides in the following folder: c:\authdata\manager on the Entrust/Authority 6.0 server.

FIPS mode

To allow Entrust/Timestamp to operate when you are running Entrust/RA and Entrust/Authority in FIPS mode, do the following:

1. Copy the default entrust.ini into a new, separate folder (or rename it to, for example, entrust.timestamp.ini).
2. Locate the FIPS section and set FipsMode to 0.

   ```
   [FIPS Mode]
   FipsMode=0
   ```

3. Run the Entrust/Timestamp configuration applet from the Windows Control Panel and set the *Location of entrust.ini file* field to point to the file created in Steps 1 and 2.

Documentation issues

PDF printing and viewing online Help

The first time you access the online help from Entrust/Authority Master Control, you'll be asked to accept or decline the Adobe Acrobat license agreement. If you do not accept the agreement, you can't view the help.

If you are a registered user of the Entrust Support Extranet and have a support agreement, you can access the following product documentation through the Entrust Support Extranet:

- *Entrust/Timestamp 4.0 User Guide* and *Release Notes*
- *Entrust/PKI 6.0 Cryptographic Hardware Guide*

To register to use the Entrust Support Extranet, see www.entrust.com/xtranet.

Configuring an auxiliary object class for user types not documented

The user.templates file (accessed through Entrust/RA) is used to populate user Directory attributes and Distinguished Name formats (refer to *Administering Entrust/PKI 6.0 on Windows* for more information on this feature). When an attribute is included in a template, you can configure an auxiliary object class that must be added to the Directory entry in order for the schema to allow the attribute within the Directory entry contents. The format for this configuration in the templates is as follows:

```
1=Internet Email Address,mail,2,1,1,rfc822MailUser
```

The example shows an attribute definition in the template file. The last item on the line defines the auxiliary object class "rfc822MailUser" that will be added to the entry before the mail attribute will be added. If the auxiliary object class is not needed, then you can remove this part of the configuration; for example:

```
1=Common Name,cn,1,1,0
```

Installing Adobe Acrobat from the Entrust/PKI 6.0 CD

If you install Adobe Acrobat from the Entrust/PKI CD, the first time you launch the help you will receive the following error message:

"Unable to find Entrust/PKI 6.0 documentation (win_pki_admin.pdf) or unable to locate Acrobat Reader. Please make sure you have both installed on your local disk."

To solve this problem, find and accept the Adobe license agreement and launch the help.

disableDbBackup description incorrect

The description of "disableDbBackup" in the "Customizing the entmgr.ini file" section in *Administering Entrust/PKI 6.0 on Windows* is incorrect. If set to true, this setting disables the database backup for Entrust/PKI, not only the first backup, as stated. The Entrust/Authority data files are still backed up.

Correction in the "To add a new user type" section

The example provided in "To add a new user type" in *Administering Entrust/PKI 6.0 on Windows* is incorrect. If you follow the steps as written, you will receive an error when you try to use that new user type. This is due to the omission of the "surname" attribute, which is a mandatory attribute for iNetOrgPerson.

Substitute the following example:

```
[Internet User]
id=3
count=2
Structural Object Class=inetOrgPerson
description=Internet User
0=Common Name,cn,1,0,1
1=Surname,sn,2,1,0
```

Hardware-based database protection note

The "Hardware-based database protection" topic in *Administering Entrust/PKI 6.0 on Windows* should state that hardware-based database protection provides stronger protection for the encrypted fields in the CA database, including private keys. Some fields, such as user DNs, are not encrypted, so the database, backups, and replications of the database should be treated as sensitive if user DNs, are confidential in your environment.

Adding new client-side settings to the certificate definitions file

The section entitled "Adding new client-side settings to the certificate definitions file" in *Installing Entrust/PKI 6.0 on Windows* is incorrect. Disregard this section and procedure.

Misinformation in the Canceling a Change DN section

The topic "Canceling a Change DN" in *Using Entrust/PKI 6.0 on Windows* is inaccurate. The text reads:

"When you cancel a DN change, the user becomes a Non-Entrust user. The user must be reactivated once again to use an Entrust-Ready application. This means that the user must enter the new activation codes generated by a Reactivate operation in order to start over."

This is not correct. When a Cancel Change DN occurs, the new entry becomes a Non-Entrust user; however, the original user DN entry is now Active and can now use Entrust as usual.

Secure Delivery SMTP not supported in Entrust/PKI 6.0

Administering Entrust/PKI 6.0 on Windows refers in error to the Secure Delivery SMTP policy setting. This setting is not supported in Entrust/PKI 6.0.

HTML help issues

- The context-sensitivity in the online help for Entrust/RA depends on java and javascripts built into the help. If your web browser is set to a high security level, the context-sensitivity may not work.
- To run the Entrust/RA online help, Microsoft Internet Explorer requires the Microsoft Virtual Machine to be installed on the machine hosting Entrust/RA. If you do not have the Microsoft Virtual Machine installed, you can either download it from the Microsoft Web site, or order it on CD from Microsoft.

Correction to "Customizing the initialization files"

Page 545 of *Administering Entrust/PKI 6.0 on Windows* in the section [User Attribute Cert] refers in error to an entry called "Attribute name". This entry is actually called "Attribute".

Change to [login] section of the entmgr.ini file

By default, the restore to Directory still stops after 1000 errors, but you can change this number by adding the maxRestoreErrors setting to the [login] section of the entmgr.ini file.

For example,

```
maxRestoreErrors=4000
```

will allow 4000 errors to occur before the restore to Directory is stopped.

Compatibility issues

Client compatibility with Directories using utf8 character sets

In a multi-Directory configuration, if the LDAP v2 Directories support the Latin-1 character set and the LDAP v3 Directories support utf8 (international) character sets, client applications will behave in an identical manner. However, if the Directories are not configured for these character sets, Entrust/Authority and the client applications should be configured to work with the same LDAP version. If upgrading an existing infrastructure operating in LDAPv2, it may be necessary to preserve LDAPv2 as the default protocol for the upgraded PKI and clients. For sites performing a first-time installation using Entrust products, LDAP v3 is recommended.

Entrust/VPNConnector 5.0 cannot be used with Entrust/PKI 6.0.1 with Microsoft Active Directory

Entrust/VPNConnector 5.0 and 5.0 SP1 cannot be used with Entrust/PKI 6.0.1 with Microsoft Active Directory. Entrust/VPNConnector creates Directory entries for VPN devices and Microsoft Active Directory does not support multi-valued relative distinguished names that some VPN devices require. Furthermore, the Directory schema required by Entrust/VPNConnector cannot be defined due to naming restrictions in Microsoft Active Directory.

If you are installing Atalla after installing Entrust/PKI

If you are installing Atalla software after you have installed Entrust/PKI 6.0.1, you may see the following message:

```
There is no evidence that Entrust/PKI has been installed on your system.
When you install Entrust/PKI replace the entmgr.ini file in the
tools\config subdirectory with the one that was written to your TEMP
directory.
```

If you see this message, you will need to open the file in the TEMP directory, copy its contents and *append* them to the existing text in /authdata/manager/entmgr.ini. You can do this with any text editor, for example, Notepad.

The lines to be copied resemble the following:

```
[Entrust Settings]
CryptokiLibraryNT=C:\Program Files\Entrust\Entrust Atalla
Interface\atpkcs11.dll
```

Client and other product compatibility issues

For more information about client compatibility issues that may affect release 5.0.x, 5.1 and 6.0 clients, refer to the release notes that ship with Entrust/Toolkit and Entrust Desktop Solutions.

Advanced capabilities in the 5.0, 5.1, and 6.0 releases that impact compatibility for prior releases are as follows: RSA-2048, ECDSA CA signing, Strict Hierarchy, CA Key Rollover, Move user, Microsoft Active Directory, Single Key Pair.

ECDSA CA keys are compatible with 5.x clients for some algorithms but not all. The "Named elliptic curves" section in *Administering Entrust/PKI 6.0 on Windows* describes the curves that are not supported with 5.x clients.

Single Key Pair only works for 6.0 clients with Release 6.0 or later PKI.

Entrust/PKI 5.0, 5.1 and 6.0 end user policies, excluding password rules, are not used by Entrust/PKI 4.0 clients.

It is suggested that 5.0.x, 5.1 and 6.0 clients use the CMP protocol (Authority=) in the entrust.ini file. This is especially true if using the advanced capabilities available in the 5.0 or later releases of Entrust/PKI.

If you plan to use any Entrust 4.0 clients or 4.0 products (Entrust/Timestamp 4.0, Entrust/VPNConnector 4.1, Entrust/WebConnector 4.0) you must take the following steps, because 4.0 compatibility is no longer specified during installation, it must be set after first-time initialization:

1. Set the CompatLevel to 4 in entsh (this allows Entrust/Authority to publish the old attribute certificate, and to accept SEP requests from version 4 clients).
2. Make sure that the Directory schema supports the attributeCertificate attribute in the CA entry described in http://www.entrust.com/resourcecenter/pdf/directory_schema_6.pdf.
3. Do not use any of the advanced capabilities and algorithms that are supported with

Entrust/Authority 5.0, 5.1 and 6.0.

4 Do not use DN encodings that are not supported (for example, UTF-8).

Product compatibility table

The products and product releases listed below are fully compatible. Unless stated otherwise, compatibility applies to all variants of each product.

This product ...	is compatible with ...
Entrust/Admin 3.0	Entrust/Manager 3.0c1.
Entrust/Admin 4.0	Entrust/Authority 4.0.
Entrust/RA 5.0	Entrust/Authority 5.0 (all configurations).
Entrust/RA 5.1	Entrust/Authority 5.1 (all configurations).
Entrust/RA 6.0	Entrust/Authority 6.0 (all configurations).
Entrust/RA 6.0.1	Entrust/Authority 6.0.1 (all configurations).
Entrust/Manager 2.1 cross-certificates	Entrust/Manager 3.0c1.
Entrust/Manager 3.0c1 cross-certificates	All releases of Entrust/Manager and Entrust/Authority, with the exception of Entrust/Authority when configured as a subordinate Certification Authority (CA).
Entrust/Authority 4.0 cross-certificates	All releases of Entrust/Manager and Entrust/Authority, with the exception of Entrust/Authority when configured as a subordinate CA.
Entrust/Authority (SEP) cross-certificates	All releases of Entrust/Manager and Entrust/Authority, with the exception of Entrust/Authority when configured as a subordinate CA.
Entrust/Authority (CMP) cross-certificates	Entrust/Authority 5.0, 5.1, and 6.0, except when configured as a subordinate CA.
Entrust/Admin 4.0 Toolkit	Entrust/Manager 3.0c1 and Entrust/Authority 4.0.
Entrust/RA Toolkit 5.0 and 5.0.1	Entrust/Authority 4.0, 5.0, 5.1 and 6.0 (note that some functionality will not be available against Entrust/Authority 5.1 and Entrust/Authority 6.0).
CMS 4.0 Toolkit (PKIX client)	Entrust/Authority 4.0. Compatible with Entrust/Authority 5.0, 5.1, 6.0 when 4.0 compatibility is specified and the advanced features aren't used. Not compatible with Entrust/Authority 5.0, 5.1, 6.0 when configured as a subordinate CA.
CMS 4.0 Toolkit (PKIX RA)	Entrust/Authority 4.0. Compatible with Entrust/Authority 5.0, 5.1, 6.0 when 4.0 compatibility is specified and the advanced features aren't used. Not compatible with Entrust/Authority 5.0, 5.1, 6.0 when configured as a subordinate CA.
Entrust/Client 3.0 (SEP)	Entrust/Manager 3.0c1, Entrust/Authority 4.0. Compatible with Entrust/Authority 5.0, 5.1 and 6.0 when 4.0 compatibility is specified and Entrust/Authority is configured as a root CA.
Entrust/Entelligence 4.0 (SEP)	Entrust/Manager 3.0c1, Entrust/Authority 4.0. Compatible with Entrust/Authority 5.0 , 5.1, and 6.0 when 4.0 compatibility is specified during installation and Entrust/Authority is configured as a root CA.

This product ...	is compatible with ...
Entrust/Entelligence 5.0 (SEP, Manager=)	Entrust/Manager 3.0c1, Entrust/Authority 4.0. Compatible with Entrust/Authority 5.0, 5.1 and 6.0 (except Microsoft Active Directory) when Entrust/Authority is configured as a root CA.
Entrust/Entelligence 5.0 (CMP, Authority=)	All configurations of Entrust/Authority 5.0, 5.1, and 6.0 (except with Microsoft Active Directory).
Entrust/Entelligence 5.0.2 (SEP, Manager=)	Entrust/Manager 3.0c1, Entrust/Authority 4.0. Compatible with Entrust/Authority 5.0, 5.1 and 6.0 (except Microsoft Active Directory) when Entrust/Authority is configured as a root CA.
Entrust/Entelligence 5.0.2 (CMP, Authority=)	All configurations of Entrust/Authority 5.0, 5.1, and 6.0.
Entrust/Entelligence 6.0 (CMP, Authority=)	All configurations of Entrust/Authority 5.0, 5.1, and 6.0.
Entrust/Profile Server 5.0 (5.0, 5.0.2, 5.1 and/or 6.0 clients)	All configurations of Entrust/Authority 5.0, 5.1 and 6.0 (except with Microsoft Active Directory).
Entrust/Profile Server 5.0.1 (5.0, 5.0.2, 5.1 and/or 6.0 clients)	All configurations of Entrust/Authority 5.0, 5.1 and 6.0 (except with Microsoft Active Directory).
Entrust/ProfileServer 5.1 (5.0, 5.0.2, 5.1 and/or 6.0 clients)	All configurations of Entrust/Authority 5.0, 5.1 and 6.0 (except with Microsoft Active Directory). If international characters (for example, Japanese characters) are used, Entrust/ProfileServer 5.1 is compatible only with Entrust Desktop Solutions 5.1 or 6.0 and Release 5.1 or 6.0 Entrust Toolkits.
Entrust/Roaming Server 6.0 (5.0, 5.0.2, 5.1 and/or 6.0 clients)	If international characters (for example, Japanese characters) are used, Entrust/Roaming Server 6.0 is compatible only with Entrust Desktop Solutions 5.1 or 6.0 and Entrust Toolkits 5.1 or 6.0.
Entrust/Timestamp 4.0	Entrust/Authority 4.0. Compatible with Entrust/Authority 5.0, 5.1 and 6.0 when 4.0 compatibility is specified and the advanced features aren't used. Not compatible with Entrust/Authority 5.0, 5.1, 6.0 when configured as a subordinate CA.
Entrust/VPN Connector 4.1	Entrust/Authority 4.0. Compatible with Entrust/Authority 5.0, 5.1 and 6.0 when 4.0 compatibility is specified and the advanced features aren't used. Not compatible with Entrust/Authority 5.0, 5.1, 6.0 when configured as a subordinate CA.
Entrust/VPN Connector 5.0	Entrust/Authority 4.0, 5.0.1, 5.0.2, 5.1 and 6.0 (except with Microsoft Active Directory).
Entrust/Web Connector 4.0	Entrust/Authority 4.0. Compatible with Entrust/Authority 5.0, 5.1 and 6.0 when 4.0 compatibility is specified and the advanced features aren't used. Not compatible with Entrust/Authority 5.0, 5.1, 6.0 when configured as a subordinate CA.
Entrust/Web Connector 5.1	Entrust/Authority 4.0, 5.0.1, 5.0.2, 5.1 and 6.0.
Entrust/Commerce Connector 4.1	Entrust/Authority 4.0.
Entrust/DeviceConnector 5.1	Entrust/Authority 5.1 and Entrust/Authority 6.0.

This product ...	is compatible with ...
AutoRA 5.0.1, 5.0.2	All configurations of Entrust/Authority 5.0, 5.1 and 6.0 (except with Microsoft Active Directory).
AutoRA 6.0	All configurations of Entrust/Authority 5.0, 5.1 and 6.0.
Entrust/TruePass 5.1	Entrust/Authority 5.1 and 6.0 (except with Microsoft Active Directory, since Entrust/ProfileServer 5.1 does not support Microsoft Active Directory).
Entrust/TruePass 6.0	All configurations of Entrust/Authority 5.0, 5.1 and 6.0.

Entrust/PKI 6.0 and Microsoft interoperability road map

The following is a road map for current information on Entrust/PKI 6.0 interoperability with Microsoft Active Directory and Microsoft PKI-enabled applications. For updates to this list, please check the Entrust Customer Support Extranet. You must have an account to access this portal. You can sign up for an account at www.entrust.com/xtranet/support/.

D = Entrust product documentation
W= Entrust white paper

Planning an installation with Active Directory	W	*Schema Requirements for Entrust/PKI 6.0 with Microsoft Active Directory*
	W	*Microsoft Active Directory Integration: Permission Configuration Guide For Entrust/PKI 6.0*
	W	*Cross-Domain Client Configuration for Entrust/PKI 6.0 with Microsoft Active Directory*
Migrating to Active Directory	W	*A strategy for migrating from an X.500 Directory to Active Directory with Entrust/PKI 6.0*
Configuring Active Directory for use with Entrust/PKI 6.0	D	*Installing Entrust/PKI 6.0 on Windows* – Chapter 2, "Configuring Microsoft Active Directory for Entrust/PKI"
		Using Microsoft Active Directory with Entrust/PKI 6.0
Installing Entrust/PKI 6.0 with Active Directory	W	*Using Microsoft Active Directory with Entrust/PKI 6.0*
	D	*Installing Entrust/PKI 6.0 on Windows*
Administering users with Active Directory	W	*Using Microsoft Active Directory with Entrust/PKI 6.0*
Customizing Directory Search Capabilities for Active Directory	D	*Installing Entrust/PKI 6.0 on Windows* – Chapter 4, "Setting up the Certification Authority (CA)" (see the section "About searchbases")
Producing CRLs	W	*Entrust/PKI 6.0: Interoperating with Microsoft PKI-enabled applications*
Setting up referrals	W	*Cross-Domain Client Configuration for Entrust/PKI 6.0 with Microsoft Active Directory*
	W	*Entrust/PKI 6.0: Interoperating with Microsoft PKI-enabled applications*
	W	*Using Microsoft Active Directory with Entrust/PKI 6.0*

Cross-certifying with other CAs	W	*Using Microsoft Active Directory with Entrust/PKI 6.0*
	W	*Entrust/PKI 6.0: Interoperating with Microsoft PKI-enabled applications*
	D	*Administering Entrust/PKI 6.0 on Windows* – Chapter 6, "Cross-certifying with other CAs", and Chapter 7, "Creating a hierarchy of CAs"
Exporting certificates to Microsoft CryptoAPI	W	*Entrust/PKI 6.0: Interoperating with Microsoft PKI-enabled applications*
	D	*Using Entrust/PKI 6.0 on Windows* – Chapter 5, "Administering individual users" (see the section "Allowing profile export")
	D	*Entrust Desktop Solutions Administrator's Guide* – Chapter 3, "Administering Entrust/Entelligence" (see the section "Export Management")

Trademark information

Entrust's partnerships with vendors that have key expertise, products and services are helping us secure the enterprises and operations of our customers in a way that meets their needs and compliments their business processes. For a complete list of all Entrust partners, see www.entrust.com/partners.